ISA 402 & ISAE 3402 Lessons Learned

Berthing, Hans Henrik

Publication date:
2013

Document Version
Early version, also known as pre-print

Verifica

ISAE 3402/ISA 402 Lessons Learned

Partner Hans Henrik Berthing,
Statsautoriseret Revisor, CIA, CGEIT, CRISC, CISA

Agenda

- Background ISA 402 & ISAE 3402
- ISA 402 Entity Users Auditor
- Period covered by audit report and period after the audit report
- Service auditors responsibilities
- Internal Audit
- Management of service organizations
- System description & Control objectives
- Subservice organizations
- ISAE 3402 >< ISAE 3000 and ISRS 4400

Hans Henrik Berthing

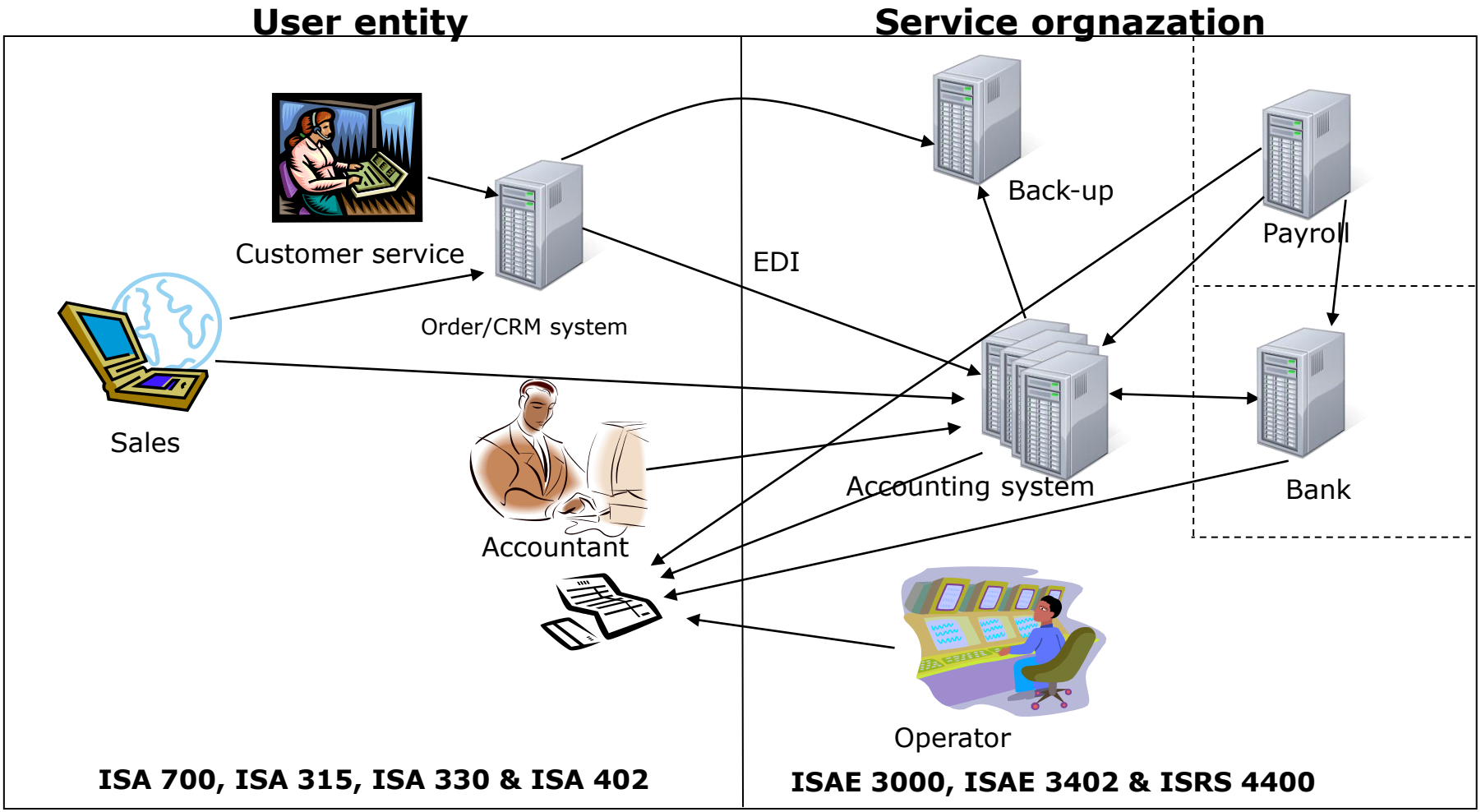
- Married with Louise and dad for Dagmar and Johannes
- CPA, CRISC, CGEIT, CISA and CIA
- ISO 9000 Lead Auditor
- Partner and owner for Verifica
- Financial Audit, since 1994 and IT Assurance since 1996
- Member of FSR IT Advisory Board
- Instructor, facilitator and speaker
- Senior Advisor & Associated professor Aalborg University (Auditing, Risk & Compliance)

Why service audit reports

Many business events have altered the landscape since the issuance of Service Audit Reports

- Increased outsourcing including usage of shared service centers
- Continued globalization and global processing models
- Increased regulation and enhanced risk management requiring service organization customers to obtain controls comfort related to outsourced activities impacting their financial statements, regulatory requirements and overall business risk management
- SAS No. 70 has served as the de facto standard on reporting on controls at a service organization on a global basis. In DK RS3411
- Other territories have steadily sought to adopt their own service
- Absence of a global standard(s) complicates engagements that cross borders
- Potential to take advantage of differing provisions within various third party control standards

User entity and service organization



Verifica

ISA 402 and ISAE 3402

A single service provided by a service organization can have direct relevance to the quality of financial reports prepared by entities around the globe. Effective controls for delivering the service are therefore essential. This new standard sets a global benchmark for reporting on controls at a service organization, thereby helping to fulfill the needs of those who use such services and their auditors under International Standards on Auditing.

IAASB Chair Arnold Schilder

- **A service auditor's standard—A new standard that will guide service organization auditors in the conduct of an** examination of, and the resultant reporting on, controls at a service organization
- **A user auditor's standard—An auditing standard that will guide user auditors in consideration of internal control** when processing is performed by a service organization

Background

- In auditing a user entity's financial statements, the user auditor needs to obtain evidence to support assertions in the user entity's financial statements that are affected by information provided by the service organization.
  - User entity is able to implement controls at the user entity over the service performed by the service organization.
  - User entity relies on the service organization to initiate, execute, and record the transactions.
- Visit the service organization and test the service organization's controls that are relevant to the user entity's internal control over financial reporting .
- Another alternative is for the service organization to give a ISAE3402 Audit Report, which report on the fairness of the presentation of the description, the suitability of the design of the controls, and in certain engagements, the operating effectiveness of the controls.

Perspective of the User Entity

Whether driven by regulatory requirement or by the board of directors focusing on corporate governance, the design and implementation of internal control over financial reporting have become key responsibilities for management.

This trend toward strong internal control has occurred simultaneously with a continuing trend to outsource functions that may be significant to an organization's operations. As a result, many enterprises have found that they have transferred the performance of many of their key controls to third-party service organizations. However, while the execution of these controls can be outsourced, management's responsibility for maintaining an effective system of internal control cannot be outsourced.

User Auditor Standard (ISA 402)

- International Standard on Auditing No. 402 (ISA 402), *Audit Considerations Relating to an Entity Using a Service Organization. This ISA deals with the user* auditor's responsibility to obtain sufficient, appropriate audit evidence when a user entity uses the services of one or more service organizations.
- Expands on how the user auditor obtains an understanding of the user entity, including internal control relevant to the audit, sufficient to identify and assess the risks of material misstatement and in designing and performing further audit procedures responsive to those risks.
- The use of a report on the controls of a service organization should provide the user auditor with an understanding of the nature and significance of the services provided and the relevant impact to the audit in identifying and assessing the risks of material misstatement.

Two Types of Engagements

Two types of engagements by service auditor:

- A type 2 engagement in which the service auditor reports on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.
- A type 1 engagement in which the service auditor reports on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

Type 1 or Type 2 Report

- The user entity should note whether the ISAE 3402 report is a Type 1 report or a Type 2 report.
  - Type 2: Controls operated effectively during the specified period of time.
  - Type 1: Do not address the operating effectiveness of controls, nor do they provide an opinion throughout a period of time.
- Type 2 report is generally preferable (unless the user entity wants only to understand the nature of the controls at the service organization and whether they are adequately designed).
- Type 2 report is necessary if the user auditor plans to use the report for reliance on internal control or the report is to be used by user entity management or the user entity's auditor for the assessment of internal control over financial reporting.

Period of Coverage

- The Type 2 report opinion clearly identifies the period of coverage.
- Less than six months of the fiscal year: Likely need to obtain an updated report or perform additional testing to complete the user entity's assessment of internal control over financial reporting.
- Period of coverage is not near the user entity's year end: Consider additional testing of controls at the service organization.
- Elapsed time between the end of the period of coverage and the user entity's year end: Consider a representation letter ("bridge letter") from the service provider.
  - Significantly changed since the most recent ISAE 3402 report,
  - Management is aware of any design or operational control deficiencies during the interim period,
  - Any other changes or matters that may affect the conclusions within the ISAE 3402 report.

Complementary user entity controls

An ISAE 3402 report identifies the controls designed to achieve the control objectives, including potential controls that the service organization intends for the user entity to implement (referred to as "complementary user entity controls").

While the specified controls should address the risks that threaten the achievement of the control objective for most user entities, individual user entity needs may vary.

As a result, user entities should consider the risks that would threaten the achievement of the control objectives from the perspective of the user entities and consider whether the controls identified adequately address those risks.

If the user entity believes that any risks are not addressed by the service organization's controls, the user entity should discuss those risks with the service organization.

Evaluate the Service Auditor Tests of Controls

- The service auditor designs tests of controls to meet the needs of the typical user entity
- Professional opinions may vary on the sufficiency of tests of controls
- Focus on the key controls that achieve the control objectives and consider whether the tests performed by the service auditor are sufficient to evaluate the effectiveness of the controls
- Evaluate service auditor's professional competence and independence from the service organization
- Certain control testing techniques inherently provide more assurance.
  - Reperformance of a control generally > inquiry and observation.
  - Independent tests of controls by the service auditor > than tests performed by internal audit

Contracts

- User entities may need or choose to, modify their contracts with the service organizations as the standards that are being reported undergo change.
- Question to ask is whether the current contract requires that a specific type of Audit report is required, eg. RS3411 (DK) report be provided at least annually. If so, user entities may want to discuss this with their legal counsel and others to determine whether a new contract is needed or whether an addendum to the current contract is possible to modify the terms to accommodate the new reporting requirements

Requirements for a service auditors engagement

- Obtain a written assertion from management of the service organization about the subject matter of the engagement.
- Type 2 engagement obtain a written assertion by management about whether in all material respects, and based on suitable criteria
  - Management's description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period,
  - The controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives, and
  - The controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives.
- Not use evidence obtained in prior engagements
- The service auditor's examination report must contain specific elements

Service Auditor use of Internal Audit

- Service auditor permitted to use the work of an internal audit function.
- Must comply with the requirements in the Standards that provide guidance to the service auditor.
- Type 2 reports required to describe the work performed by the internal audit function, and procedures used to test that work.
  - Narrative description summarizing the processes tested by internal audit, the nature of the work performed and the procedures performed by the service auditor to test that work. This description can be provided in the introduction to the service auditor test section
  - Attribution of individual tests in the service auditor's testing section of the report to internal audit, along with a description of the specific procedures performed by the service auditor to test the work of internal audit
- Internal auditors direct assistance to the service auditor, planned and supervised by the service auditor, need not to be disclosed.

Service organization responsibilities

Service organizations have five primary responsibilities:

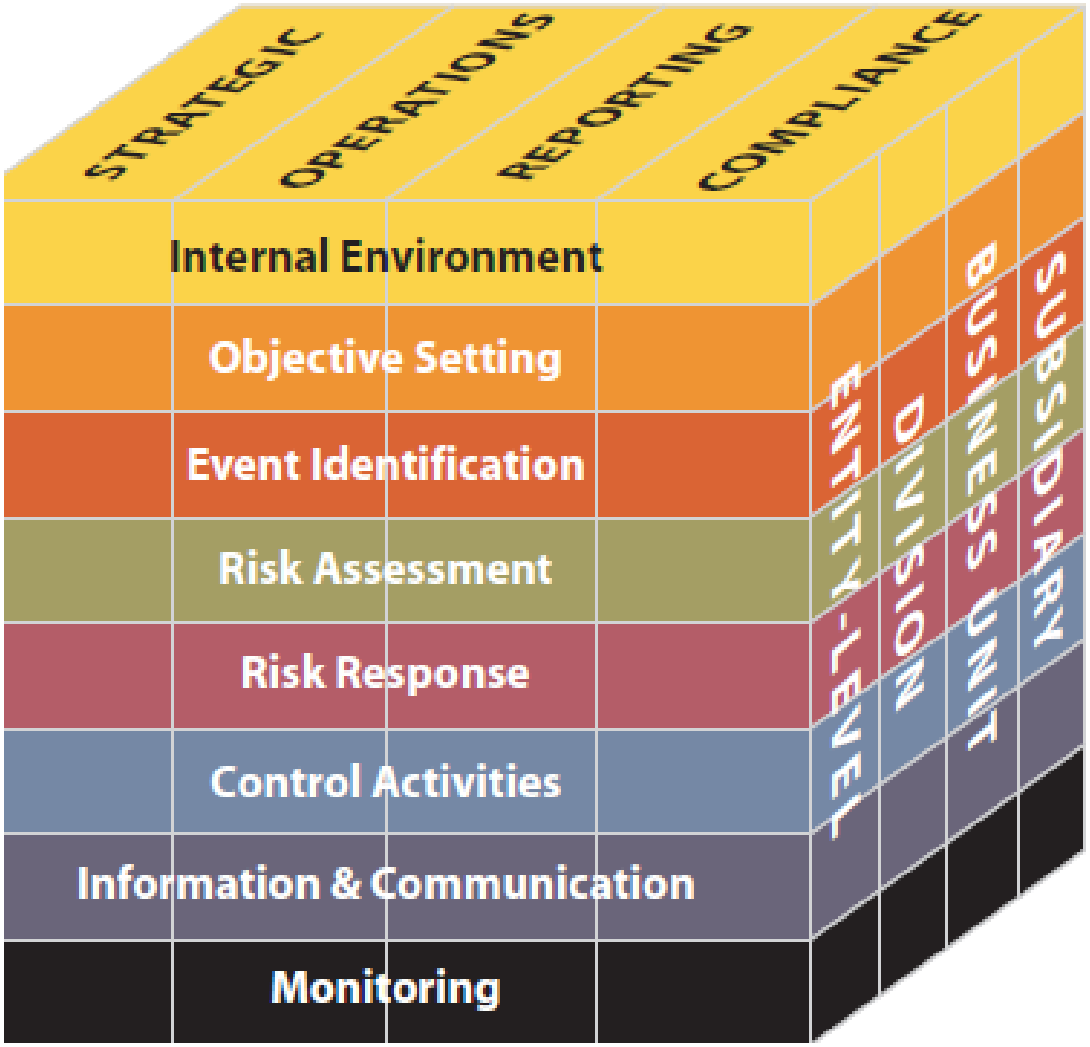
1. Prepare and present a complete an accurate description of the system
2. Specify the control objectives of the system and state those control objectives in the description of the system
3. Identify the risks that threaten the achievement of the control objectives (although these risks are not included in the service organization report)
4. Design, implement and maintain controls to provide reasonable assurance that the control objectives will be achieved
5. Provide a written assertion to accompany the description as to the completeness and accuracy of the information provided and state the criteria used as a basis for making the assertion

Describing the service organization's system

The service organization's description of its system includes:

- Description of the services provided, including classes of transactions processed.
- Description of the procedures by which services are provided, including transaction initiation, authorization, recording, processing and correction..
- Description of the capturing of significant events and conditions other than transactions.
- Description of the process used to prepare reports or information provided to user entities.
- Description of control objectives and related controls, including complementary user entity controls.
- Description of aspects of the service organization's control environment, risk assessment process, information and communications systems, control activities and monitoring controls. (known from ISA 315)

ERM - COSO



Other responsibilities

Management's written assertion in the report. The assertion is a separate component of the report, signed by management. The assertion communicates:

- Service organization management's responsibility for the description of the system
- Achievement of the evaluation criteria of the description of the system
- Identifying risks that threaten the achievement of the control objectives. The New Standards require the service organization to support its assertion by:
- Identifying the risks that threaten the achievement of the control objectives
- Determining whether the controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives from being achieved

Management Assertion

- Assertion would accompany description of service organizations description of controls
- Management is responsible for selecting criteria, for determining whether it is appropriate, and it muse be available to the intended users
- Nature, timing and extent of service auditor procedures would be expected to be the same
- IAASB believes assertion-based engagements are more appropriate because of the explicit acknowledgement by management of its responsibility for the matters contained within the assertion
- IAASB specifically sought perspective where situations may arise where it isn't possible or practicable for management to provide an assertion

Subservice organizations

- A subservicer is a service organization used by another service organization
- "Carve-out" or "inclusive" methods are available for dealing with services provided by subservice organizations in the report.
- Identify all subservice organizations that affect user entities' financial statements.
- Does subservice organizations have existing service organization reports or would be willing to provide one to your customers. (Cheaper and easier to provide your customers with a copy and limit your report to only your processes).
- Discuss reporting strategy with subservice organization.
- Assistance and cooperation with the subservice organization
- Obtain agreement with your subservice organization regarding strategy, and get this agreement in writing.
- If you are a subservice organization, discuss with the primary service organization how the needs of their clients will be met.

Inclusive subservice organizations

- If a service organization wishes to include a description in the report of a subservice organization's role and controls (inclusive method), the subservice organization must prepare a management assertion report similar to the assertion report prepared by the service organization's management
- Getting subservice organization management to agree to provide this assertion may be more difficult than obtaining a letter of representations.

Carve out method

- Nature and functions of the subservice organization are described,
- Control activities performed by the subservice organization are not included in the description of controls of the system.
- Use of the carve-out method of reporting is common,
- With the standards requiring an assertion when using the inclusive method, might be an increased use of the carve-out method
- User entities should give thorough deliberation to the types of services that are being carved out and how they relate to the user entity.
- Extent of interaction between the subservice organization and the service organization
  - Subservice organization has a service auditor report performed,
  - User entity is able to obtain the service auditor report
  - Additional procedures/oversight is needed related to the services being provided by the subservice organization

Other audit reports

- ISAE 3402
- ISAE 3000
- ISRS 4400

Summary

- Plan the audit both user entity and Service Organization
- Timing of the audit report
- Description of system including control objectives and controls
- Complimentary controls
- Subservice organizations
- Service auditors competence and independence
- Standards used by service organizations and Service Auditor

Questions

Hans Henrik Berthing, Statsautoriseret revisor

| CGEIT | CRISC | CISA | CIA

Phone +45 35 36 33 56 |

Mobile 22 20 28 21 |

E-mail hhberthing@verifica.dk

Verifica

Statsautoriseret Revisionsvirksomhed